ITCertTest

ITCERTTEST
IT Exam study guide / simulations

http://www.itcerttest.com

IT exam study guide / simulations

Exam : **FCP_FGT_AD-7.4-JPN**

Title : FCP - FortiGate 7.4 Administrator (FCP_FGT_AD-7.4日本語版)

Vendor : Fortinet

Version : DEMO

QUESTION NO: 1
展示品を参照してください。

IPS diagnostic output

```
# diagnose test application ipsmonitor

1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
6: Submit attack characteristics now
10: IPS queue length
11: Clear IPS queue length
12: IPS L7 socket statistics
13: IPS session list
14: IPS NTurbo statistics
15: IPSA statistics
...
97: Start all IPS engines
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

図に示されている侵入防止システム (IPS) 診断コマンドを調べます。
オプション 5 を IPS 診断コマンドで使用し、結果として CPU
使用率が減少した場合、正しい結論は何ですか?
A. IPS エンジンがすべてのトラフィックをブロックしています。
B. IPS エンジンは大量のトラフィックを検査しています。
C. IPS エンジンは侵入攻撃を防ぐことができません。
D. IPS エンジンは通常の状態で動作を続けます。
Answer: B
Explanation:
If there are high-CPU use problems caused by the IPS, you can use the diagnose test application ipsmonitor command with option 5 to isolate where the problem might be. Option 5 enables IPS bypass mode. In this mode, the IPS engine is still running, but it is not inspecting traffic. If the CPU use decreases after that, it usually indicates that the volume of traffic being inspected is too high for that FortiGate model.

QUESTION NO: 2
ファイアウォール
ポリシーとウイルス対策プロファイルの構成を示す展示を参照してください。

感染したファイルを初めてダウンロードするときに、ユーザーがブロック置換メッセージを受信できないのはなぜですか?

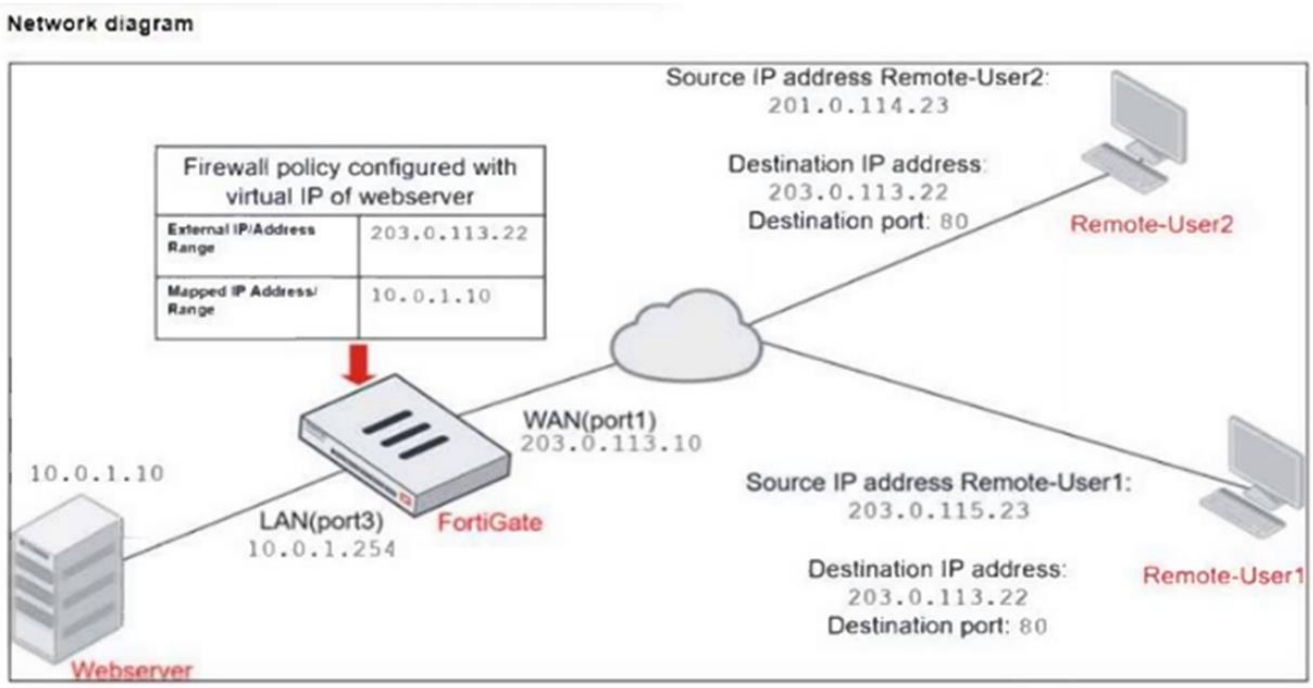
A. フローベースの検査モードを使用する場合は、侵入防止セキュリティ
プロファイルを有効にする必要があります。
B. 検査のためにファイルを FortiSandbox に送信するオプションが有効になっています。
C. ファイアウォール ポリシーは、ファイルに対して完全なコンテンツ検査を実行します。
D. フローベースの検査が使用され、最後のパケットがユーザーにリセットされます。
Answer: D
Explanation:
In flow-based inspection mode, FortiGate sends a reset (RST) packet to the client instead of providing a replacement message, which causes the block message not to be displayed.

QUESTION NO: 3
FortiGate の等コスト マルチパス (ECMP) 構成に関する次の 2
つの記述のうち、正しいものはどれですか? (2 つ選択してください。)
A. SD-WAN が有効になっている場合は、パラメータ load-balance-mode
を使用して負荷分散アルゴリズムを制御します。
B. SD-WAN が無効になっている場合は、パラメータ v4-ecmp-mode
をボリュームベースに設定できます。
C. SD-
WANが有効になっている場合、距離と優先度の値が等しくないルートをECMPの一部として設定できます。
D. SD-WAN
が無効になっている場合は、構成システム設定で負荷分散アルゴリズムを構成します。
Answer: A,D
Explanation:
When SD-WAN is enabled on FortiGate, the load balancing algorithm for Equal-Cost Multi-Path (ECMP) is configured using the load-balance-mode parameter under SD-WAN settings. However, if SD-WAN is disabled, the ECMP load balancing algorithm can be configured under config system settings. This flexibility allows FortiGate to control traffic routing behavior based on the network configuration and requirements.
Reference:
FortiOS 7.4.1 Administration Guide: ECMP Configuration

QUESTION NO: 4
FortiGate でサポートされている IPsec IKEv1 認証の機能はどれですか (2
つ選択してください)。
A. 認証方法としての事前共有キーと証明書署名
B. 拡張認証 (XAuth) リモートピアにユーザー名とパスワードの提供を要求する
C. 交換されるパケット数が少なくなるため、認証が高速になる拡張認証 (XAuth)
D. 認証方法として証明書署名を設定する場合、リモートピアに証明書は必要ありません。
Answer: A,B
Explanation:
FortiGate supports both pre-shared key and certificate signature methods for IKEv1 authentication. These methods provide flexibility depending on the security requirements of the network. Additionally, FortiGate supports Extended Authentication (XAuth), which

requests a username and password from the remote peer, enhancing security by adding an extra layer of authentication. The XAuth method does not necessarily make the authentication faster; it is an additional security measure.
Reference:
FortiOS 7.4.1 Administration Guide: IPsec VPN Configuration

QUESTION NO: 5
展示品を参照してください。



Firewall policies

ID	Name	Source	Destination	Schedule	Service	Action
WAN (port1) → LAN (port3) 2						
4	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_access	all	Webserver	always	ALL	ACCEPT

展示品には、ネットワークに接続された FortiGate
デバイスの図とファイアウォールの構成が示されています。
管理者は、Remote-User2 の Web サーバー
アクセスを拒否するデフォルト設定の拒否ポリシーを作成しました。
このポリシーは、Remote-User1 が Web サーバーにアクセスできるようにし、Remote-User2 が Web サーバーにアクセスできないようにするように機能する必要があります。
管理者は、Remote-User2 の Web サーバー
アクセスを拒否するために、ポリシーに対してどの 2
つの構成変更を行うことができますか? (2 つ選択してください。)

A. 拒否ポリシーで match-vip を有効にします。
B. 拒否ポリシーで宛先アドレスを Web サーバーとして設定します。
C. 拒否ポリシーで match-vip を無効にします。
D. Allow_access ポリシーで宛先アドレスを Deny_IP として設定します。

Answer: A,B

Explanation:
To deny access to the web server for Remote-User2 while allowing Remote-User1 to access the same web server, two configuration changes can be made:
Enable match-vip in the Deny policy:
By enabling the match-vip option in the Deny policy, the FortiGate will check for virtual IP (VIP) objects during policy matching. This setting allows the firewall policy to correctly identify and block traffic directed to a specific mapped IP address, such as the web server, when using a VIP configuration.
Set the Destination address as Webserver in the Deny policy:
Setting the Destination address to "Webserver" in the Deny policy ensures that the policy specifically targets traffic attempting to reach the web server. This configuration helps to precisely control which traffic should be blocked, focusing the Deny policy on the intended destination.
Reference:
FortiOS 7.4.1 Administration Guide: Deny matching with a policy with a virtual IP applied
FortiOS 7.4.1 Administration Guide: Configuring Policies with VIPs

QUESTION NO: 6
FortiGate は FortiAnalyzer および FortiManager と統合されています。
ファイアウォール ポリシーを作成すると、機能性を向上させ、FortiAnalyzer または FortiManager
へのログの記録をサポートするために、どの属性がポリシーに追加されますか?

A. ログID

B. ポリシーID
C. (シーケンスID
D. ユニバーサルユニーク識別子
Answer: D
Explanation:
When a firewall policy is created in FortiGate integrated with FortiAnalyzer and FortiManager, a Universally Unique Identifier (UUID) is added to the policy to support logging and management.

QUESTION NO: 7
組織では、リモート ユーザーが PC 上で実行されている外部アプリケーション
データを送信し、SSUTLS 接続を介して FTP リソースにアクセスする必要があります。
どの FortiGate 構成でこの目標を達成できますか?
A. SSL VPN クイック接続
B. SSL VPN トンネル
C. SSL VPN ブックマーク
D. ゼロトラストネットワークアクセス
Answer: B
Explanation:
An SSL VPN tunnel allows remote users to securely connect to the organization's network and transmit all traffic, including external application data and FTP resources, through an encrypted SSL/TLS connection. This ensures secure access to the network while supporting various protocols such as FTP and other application-specific traffic from the user's PC.

QUESTION NO: 8
マルチ VDOM 環境でのセキュリティ
ファブリックの展開に関する次の記述のうち正しいものはどれですか。
A.
ダウンストリームデバイスは、どのVDOMからでもアップストリームデバイスに接続できます。
B. 環境内の各VDOMは、異なるセキュリティファブリックの一部になることができます。
C. デバイスが接続されたポートのない VDOM はトポロジに表示されません
D. セキュリティ評価レポートは、構成されたVDOMごとに個別に実行できます。
Answer: C
Explanation:
"When you configure FortiGate devices in multi-vdom mode and add them to the Security Fabric, each VDOM with its assigned ports is displayed when one or more devices are detected. Only the ports with discovered and connected devices appear in the Security Fabric view and, because of this, you must enable Device Detection on ports you want to have displayed in the Security Fabric. VDOMs without ports with connected devices are not displayed. All VDOMs configured must be part of a single Security Fabric."

QUESTION NO: 9
FortiGate HA 構成の同期に関して正しい記述はどれですか? (2 つ選択してください。)

A. デバイスのチェックサムが相互に比較され、構成が同じであることを確認します。
B. 増分構成同期は、プライマリ FortiGate デバイスで行われた変更からのみ実行できます。
C.
HAクラスタ内の任意のFortiGateデバイスで行われた変更から増分構成同期が発生する可能性があります。
D. 一部の構成項目が他の HA
メンバーに同期されていないため、デバイスのチェックサムは互いに異なります。
Answer: A,C
Explanation:
"After the initial synchronization is complete, whenever a change is made to the configuration of an HA cluster device (primary or secondary), incremental synchronization sends the same configuration change to all other cluster devices over the HA heartbeat link"